IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In Re Application of:	Hericourt et al.	Conf. No.:	4960
Serial No.:	10/007,750	Art Unit:	2137
Filed:	13 November 2001	Docket No.:	FR920000073US1 (IBME-0166)
Title:	METHOD AND SYSTEMS FOR USING WITH CONFIDENCE CERTIFICATES ISSUED FROM CERTIFICATE AUTHORITIES	Examiner:	Abyaneh, Alis S.

Mail Stop Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

BRIEF OF APPELLANTS

This is an appeal from the Final Rejection dated 16 October 2006, rejecting claims 1-9. This Brief is accompanied by the requisite fee set forth in 37 C.F.R. 41.20(b)(2).

REAL PARTY IN INTEREST

International Business Machines Corporation is the real party in interest.

RELATED APPEALS AND INTERFERENCES

There are no related appeals or interferences.

STATUS OF CLAIMS

As filed, this case included claims 1-9, each of which remains pending. Claims 1-9 stand rejected and form the basis of this appeal. No claims are allowed.

STATUS OF AMENDMENTS

No amendment has been submitted in response to the Final Rejection filed by the Office on 16 October 2006.

SUMMARY OF THE CLAIMED SUBJECT MATTER

The present invention provides methods for filtering certificates issued from as few as one certificate authority.

Claim 1 claims a method for filtering certificates issued from as few as one certificate authority (CA), the method comprising the steps of: receiving a certificate and storing the certificate (*see, e.g.*, pp. 9, 12, 14); preventing use of the certificate until validation (*id.*); identifying a certificate authority that has issued the certificate (*id.*); identifying a certificate authority filter by referring to a table, that comprises identification of at least one certificate authority filter (*see, e.g.*, pp. 9, 12-14); sending a request to the identified certificate authority filter (*see, e.g.*, pp. 9, 13-14); receiving from the identified certificate authority filter a response to the request, the response comprising information related to the certificate authority that has issued the certificate and a public key of the certificate authority that has issued the certificate (*see, e.g.*, pp. 9, 13-15); determining according to the response whether the certificate authority is a trusted certificate authority (*see, e.g.*, pp. 9, 12-13, 15); and validating the certificate if the

certificate authority that has issued the certificate is a trusted certificate authority (*see, e.g.*, pp. 9, 13, 15). *See also*, FIGS. 3-6.

Claim 7 claims a method, in as few as one certificate authority filter connected to a network, for filtering certificates issued from as few as one certificate authority, the method comprising the steps of: receiving a request comprising an identification of a certificate authority (*see, e.g.*, pp. 9, 21); identifying the certificate authority in said request (*id.*); finding in a table the certificate authority, the table comprising: identification of as few as one certificate authority and a level of trust and a public key associated with each of said as few as one certificate authority (*see, e.g.*, pp. 10, 21, 22); determining a level of trust of the identified certificate authority referring to said table (*see, e.g.*, pp. 10, 21); retrieving a public key associated with the identified certificate authority referring to said table (*see, e.g.*, pp. 10); and sending a response to an originator of the request, said response comprising the level of trust of the identified certificate authority and the public key associated with the identified certificate authority (*see, e.g.*, pp. 10, 21). *See also*, FIGS. 3-7.

GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

Claims 1-9 stand rejected under 35 U.S.C. §102(e) as being unpatentable over U.S. Patent No. 6,134,550 to Van Oorschot *et al.*

ARGUMENT

I. Rejection of claims 1-9 over Van Oorschot *et al.*

Appellants respectfully submit that the rejection of claims 1-9 under 35 U.S.C. § 102(e) as allegedly being unpatentable over Van Oorschot *et al.* is defective.

A. Claims 1 and 7

With respect to claims 1 and 7, Appellants respectfully submit that the Examiner has failed to give the phrase "as few as one" its proper meaning and that, as a consequence of this failure, Van Oorschot *et al.* fail to teach or suggest every feature of the claimed invention.

In the Final Office Action, the Examiner states that "'**as few as one** certificate authority' does not mean only one single certificate authority and it could be interpreted as one or more certificate authority." Final Office Action at 2 (emphasis in original). The Examiner then goes on to allege that because "Van Oorschot teaches a table including identification of individual certificate authorities, this clearly reads on the applicant's claim limitation (see column 5, lines 7-14 and column 9, lines 32-36)." *Id.*

However, as explained in Appellants' 01 August 2006 Amendment and 13 December 2006 Pre-Appeal Brief, the Examiner has misinterpreted one or both of Van Oorschot *et al.* and the present application. *See* 13 December 2006 Pre-Appeal Brief at 2-4 and 01 August 2006 Amendment at 7-9.

With respect to Van Oorschot *et al.*, the portions cited by the Examiner read, in their entireties:

> Alternatively, the certificate chain data constructing unit can provide names or directory information or other identification data of those certification authorities in a selected path between a beginning and target

> certification authority, for example the target CA being the CA which issued the certificate of a subscriber whose public key certificate is to be verified.
>
> Van Oorschot *et al.*, column 5, lines 5-13 (emphasis added).

> As another embodiment the certificate chain data 209 may represent individual certificates from the distributed memory 302 or certificate chain data 209 may represent links in a trusted path from which a certificate chain may be determined.
>
> Van Oorschot *et al.*, column 9, lines 32-36 (emphasis added).

The first quotation above makes clear that the method of Van Oorschot *et al.* requires ***at least two*** certification authorities, *e.g.*, a beginning certification authority and a target certification authority. *See* 13 December 2006 Pre-Appeal Brief at 2 and 01 August 2006 Amendment at 8; *see also* 29 December 2005 After-Final Amendment at 7-8 and 20 July 2005 Request for Reconsideration at 6. That is, the method of Van Oorschot *et al.* is inoperable and/or inapplicable in the event that a single certificate authority is involved or available.

The second quotation above fails to cure this defect and, in fact, offers no support for the Examiner's allegation that "Van Oorschot teaches a table including identification of individual certificate authorities." The quoted language relates to individual certificates, not certification authorities. In fact, as noted in Appellants' 01 August 2006 Amendment, the "certificate chain data" that represents the individual certificates comprise relationships among ***at least two*** certification authorities: "Certificate chains correspond to directed trust paths, also known as certification paths, such as trust relationships among certification authorities where at least one certification authority (CA) has certified another certification authority." Van Oorschot *et al.*, column

2, lines 22-26. *See* 13 December 2006 Pre-Appeal Brief at 3 and 01 August 2006 Amendment at 8.

Despite the above insistence by the Examiner to read the claim language "as few as one" as equivalent to "one or more," the Examiner goes on to assert that "Van Oorschot teaches a method for filtering certificates issued from as few as one certificate authority." Final Office Action at 3. As noted above, this is clearly false. The Examiner has failed to cite any portion of Van Oorschot et al. that allegedly teaches any method involving "as few as one" certificate authority.

With respect to the language of the pending claims, Appellants respectfully assert that the Examiner's interpretation of the phrase "as few as one certificate authority" as equivalent to "one or more certificate authority" and the Examiner's conclusion that the claims are therefore anticipated by Van Oorschot *et al.*, the methods of which, as described above, require at least two certificate authorities, is both factually and logically untenable. *See* 13 December 2006 Pre-Appeal Brief at 3-4, 01 August 2006 Amendment at 8-9, 29 December 2005 After-Final Amendment at 7-8, and 20 July 2005 Request for Reconsideration at 6.

Appellants assert that the phrases "as few as one" and "one or more" are not equivalent. For example, if one were to restrict a group of procedures to those operable using "as few as one step," the group would include those procedures that include only one step as well as those that include more than one step ***but which are also operable using only one step***. Contrarily, if one were to restrict the group of procedures to those operable using "one or more steps," the group would include all procedures having at least one step. That is, a procedure that is operable only when it includes two or more

steps would be excluded from the group requiring operability using "as few as one step" but would not be excluded from the group requiring operability using "one or more steps."

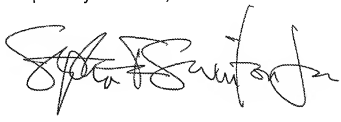
Appellants' use of the phrase "as few as one" in claims 1 and 7 is no different. The claimed methods require the ability to filter certificates issued from as few as one certificate authority. Thus, certificate filtering methods requiring data from more than one certificate authority, such as those of Van Oorschot *et al.*, are not methods for filtering certificates issued from as few as one certificate authority.

Appellants assert that, given the above distinction between "as few as one" and "one or more," none of the pending claims, each directed toward filtering certificates issued from "as few as one certificate authority," is anticipated by Van Oorschot *et al.*, which, as explained above and in Appellants' earlier responses, requires a relationship between or among certification authorities and therefore at least two certification authorities. *See* 13 December 2006 Pre-Appeal Brief at 3-4, 01 August 2006 Amendment at 8-9, 29 December 2005 After-Final Amendment at 7-8, and 20 July 2005 Request for Reconsideration at 6.

Conclusion

In summary, Appellant submits that claims 1-9 are allowable because Van Oorschot *et al.* fail to anticipate or make obvious any of the rejected claims.

Respectfully submitted,



Stephen F. Swinton, Jr.
Reg. No. 53,661

Date: 22 February 2007

Hoffman, Warnick & D'Alessandro LLC
75 State Street, 14th Floor
Albany, New York 12207
T: 518.449.0044
F: 518.449.0047

CLAIMS APPENDIX

1. A method for filtering certificates issued from as few as one certificate authority (CA), the method comprising the steps of:

receiving a certificate and storing the certificate;

preventing use of the certificate until validation;

identifying a certificate authority that has issued the certificate;

identifying a certificate authority filter by referring to a table, that comprises identification of at least one certificate authority filter;

sending a request to the identified certificate authority filter;

receiving from the identified certificate authority filter a response to the request, the response comprising information related to the certificate authority that has issued the certificate and a public key of the certificate authority that has issued the certificate;

determining according to the response whether the certificate authority is a trusted certificate authority; and

validating the certificate if the certificate authority that has issued the certificate is a trusted certificate authority.

2. The method according to claim 1 further comprising the step of:

discarding the certificate if the response indicates that the certificate authority that has issued the certificate is not a trusted certificate authority.

3. The method according to claim 1, wherein the step of identifying the certificate authority that has issued the certificate comprises the further step of:

retrieving an identification of the certificate authority from the certificate.

4. The method according to claim 1, wherein the step of sending a request to the identified certificate authority filter comprises the further step of:

including in said request an identification of the certificate authority that has issued the certificate.

5. The method according to claim 1, wherein the response received from the identified certificate authority filter comprises a level of trust assigned to the certificate authority, and wherein the step of determining according to the response whether the certificate authority is a trusted certificate authority comprises the further step of:

checking whether the level of trust assigned to the certificate authority corresponds to a level of trust of a trusted certificate authority.

6. The method according claim 1 wherein the step of validating the certificate comprises the further steps of:

comparing the public key included in the response received from the identified certificate authority filter with a public key included in a response from a second certificate authority filter; and

validating the certificate if the public key included in the response received from the identified certificate authority filter is the same as the public key received in the response from the second certificate authority filter.

7. A method, in as few as one certificate authority filter connected to a network, for filtering certificates issued from as few as one certificate authority, the method comprising the steps of:

receiving a request comprising an identification of a certificate authority;

identifying the certificate authority in said request;

finding in a table the certificate authority, the table comprising: identification of as few as one certificate authority and a level of trust and a public key associated with each of said as few as one certificate authority;

determining a level of trust of the identified certificate authority referring to said table;

retrieving a public key associated with the identified certificate authority referring to said table; and

sending a response to an originator of the request, said response comprising the level of trust of the identified certificate authority and the public key associated with the identified certificate authority.

8. The method according to claim 7 wherein said request further comprises an identification of a destination entity.

9. The method according to claim 8, wherein:

the table further includes, associated with the as few as one certificate authority, the destination entity and a level of trust associated with the destination entity; and

wherein the step of determining the level of trust further includes the step of determining the level of trust associated with the destination entity by referring to the table.

EVIDENCE APPENDIX

No evidence has been entered and relied upon in the appeal.

RELATED PROCEEDINGS APPENDIX

No decisions rendered by a court or the Board in any proceeding are identified in the related appeals and interferences section.